UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/720,054	11/25/2003	Sakari Poussa	39700-606001US/NC39911US	4194

64046 7590 07/20/2010

MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C
ONE FINANCIAL CENTER
BOSTON, MA 02111

EXAMINER	
RAHIM, MONJUR	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
07/20/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/720,054	POUSSA ET AL.	
	Examiner	Art Unit	
	MONJOUR RAHIM	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,10-12 and 14-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,10-12 and 14-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application.
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment and argument field on **26 April 2010**.

2. **Claims 14, 16, 21, 24-26** have been **amended.**

3. **Claims 1-8, 10-12, 14-26** remain **rejected**.

Responses to the Argument

4. The applicant's arguments filed on **26 April 2010** have been fully considered but they are not persuasive. In the Remarks, the applicant has argued in substance:

Argument (Page 1-4):

(a) "On page 3 of the Office Action, the Examiner alleges that Leung at col. 7, lines 33-50 discloses the following feature of claim 1 "at least one management client configured to issue, in response to communication received at said application device from a user equipment via a session key management protocol, security association management requests to create and manage, with said session key management protocol, security associations for use by said provided internet protocol security services, said at least one management client deployed in said application device." However, it is clear that the Examiner has committed a clear error by ignoring the express language of claim 1. Specifically, claim 1 recites that the "at least one management client [is] configured to issue, in response to communication received at said application device from a user equipment via a session key management protocol, security association management requests to create and manage ... security associations .... " But Leung's server at col. 7, lines 33-50 has no need to ever issue security association management requests to create and manage security associations".

(b) On pages 3-4 of the Office Action, the Examiner acknowledges that Leung fails to disclose or suggest "at least one management client deployed in said application device." To cure this gap in Leung, the Examiner relies on Yokote at paragraphs 0012 and 0066. However, a careful scrutiny reveals that those paragraphs do not disclose what the Examiner alleges. Instead, Yokote at paragraphs 0012 and 0077 generally discloses security associations but not that the "at least one management client [is] deployed in said application device." Therefore, claim 1, as well as claims 2-8, at least by reason of their dependency, are allowable over Leung and Yokote, whether taken individually, or in combination, and the rejection under 35 U.S.C. §103(a) of claims 1-8 should be withdrawn for this additional reason.

Response:

(a) Examiner respectfully disagrees with the applicant, because when a mobile node send a request to a server, then it response to the request (such as, Authentication request) according to the profile by applying security association via management key protocol. By default this protocol configured to manage/response/reply (send/receive message) in a client sever environment. Please see Leung col 7, lines 33-50.

(b) Examiner respectfully disagrees with the applicant, because "sending binding update" to the node (mobile device) is the same as deployment to the device. Please see Yokote ¶10 and ¶12.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8, 10-12 and **14-26** are rejected under **35 U.S.C §103(a)** as being unpatentable over U.S. Patent No. 6,760,444, hereinafter Leung and in view of Yokote (US Publication No. 20020157024), hereinafter Yokote.

In regard to **claim 1**, Leung discloses:

- an application device (Leung, col 6, lines 24-26).

- a service device (Leung, col2, line 58 to column 3, line 16), wherein The Home Agent is the service device.

- a communication network configured to connect said application device to said service device (Leung, col 6, lines 24-26), wherein the home agent and handheld device are connected via communication network.

- an internet protocol security service unit configured to provide one or more internet protocol security services comprising at least one of authentication services and encryption services, said internet protocol security service unit deployed in said service device (Leung, col 6, lines 24-26, col 2, lines 58 and col 3, lines 16) wherein, The Home Agent may contact the server with a request for services such as creating and managing security associations or authentication services handled by the server's internet protocol security services.

- a management server configured to receive said security association management requests issued from said at least one management client and to respond, in connection with said internet protocol security service unit, to said security association management requests received at said management server, said management server deployed in said service device The Home Agent may contact the server with a request for services such as creating (Leung, col 2, line 58, col 3, line 16) and managing security associations or authentication services (handled by the server's internet protocol security services) and receive in return a security association (Leung column 7, lines 16-32). The response is sent by the server to the home agent (Leung col 7, lines 33-50), since the security associations may comprise keys (Leung column 7, line 67), this uses a session key management protocol.

- at least one management client configured to issue, in response to communication received at said application device from a user equipment via a session key management protocol, The response is sent by the server to the home agent (Leung col 7, lines 33-50), since the security associations may comprise keys (Leung col 7, line 67), this uses a session key management protocol.

Leung does not explicitly teach **security association management requests to create and manage, with said session key management protocol, security associations for use by said provided internet protocol security services, said at least one management client deployed in said application device ;** however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based

on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶0066.

In regard to **claim 2, 11,** and **19:**

The Home Agents network interface for communicating with the communications network, see col 9, line 53 to col 10, line 6, provides communication between the management clients and the server.

In regard to **claim 3, 12, 15**

- wherein said security association is taught by Leung see figure 4, item 412. but Leung does not explicitly teach **management requests to create and manage comprise at least one of adding requests configured to add security associations, deleting requests configured to delete security associations, and querying requests configured to query about security associations;** however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the request to create and manage disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate

SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶0066.

In regard to **claim 16**, Leung discloses:

a management server configured to receive security association management requests issued from at least one management client included in an application device external to said apparatus and to respond, in connection with said internet protocol security service unit, to said received security association management requests to create and manage security associations The Home Agent may contact the server with a request for services such as creating (Leung, col 2, line 58, col 3, line 16) and managing security associations or authentication services (handled by the server's internet protocol security services) and receive in return a security association (Leung column 7, lines 16-32). The response is sent by the server to the home agent (Leung col 7, lines 33-50), since the security associations may comprise keys (Leung column 7, line 67), this uses a session key management protocol. Mobile node is the individual computing device (Abstract).

Leung does not explicitly teach **requests to create and manage** however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶0066.

In regard to **claim 4** and **5:**

the server may use IP, for which all communications inherently use sockets at both ends of a communication and data structures for the packet formats (Leung, col 6, lines 26-28 and col 8, lines 37-39).

In regard to **Claims 6, 7, 9,** and **17**:

Regarding **claim 6**, Leung does not discuss the architecture of the software in the system that is employed to use the communications interface.

Official notice is given that it is well-known in the art to package the related functions for using a device on a computer in a DLL.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the network interface functions as a DLL.

Regarding **claims 7, 9,** and **17** Leung does not disclose the structure of the network connecting the Home Agents to the servers.

Official notice is given that it is well-known in the art to implement computer connections using a local network.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Leung's invention using a local network.

In regard to **claim 8:**

Each client's security associations and communications may use a different keying algorithm (Leung, FIG.4, item 412).

In regard to **claim 10**, Leung discloses:

- providing one or more internet protocol security services comprising at least one of authentication services and encryption services from an internet protocol security service unit, said internet protocol security service unit being deployed in a service device (Leung, col 2, line 58 to col 3, line 16) The Home Agent may contact the server with a request for services such as creating and managing security associations or authentication services (handled by the server's internet protocol security services.

- receiving in a management server said security association management requests issued from said at least one management client (Leung col 7, lines 16-32), wherein receive in return a security association.

- and responding, in connection with said internet protocol security service unit, to said security association management requests received at said management server, said management server being deployed in said service device, wherein said application device is connected to said service device by a communication network Leung discloses an interaction between a Home Agent the application device comprising management clients that is connected to a server (the service device) via a communications network (Leung col 6, lines 24-26) and one or more wireless clients. The Home Agent may contact the server with a request for services such as creating (Leung col 2, line 58 to col 3, line 16) and managing security associations or authentication services (handled by the server's internet protocol security services) and receive in return a security association (Leung col 7, lines 16-32). The response is sent by the server to the home agent (Leung column 7, lines 33-50), since the security associations may comprise keys (col column 7, line 67), this uses a session key management protocol.

- issuing, in response to communication received at an application device from a user equipment via a session key management protocol (Leung, figure 4, item 412).

Leung does not explicitly teach **security association management requests to create and manage, with said session key management protocol, security associations for use by said provided internet protocol security services, from at least one management client, said at least one management client being deployed in said application device;** however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based

on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶0066.

In regard to **claim 14,** Leung discloses:

Leung discloses an interaction between a Home Agent the application device comprising management clients, that is connected to a server (the service device) via a communications network (Leung, col 6, lines 24-26) and one or more wireless clients. The Home Agent may contact the server with a request for services such as creating (Leung, col 2, line 58 to column 3, line 16) and managing security associations or authentication services (handled by the server's internet protocol security services) and receive in return a security association (Leung, col 7, lines 16-32). The response is sent by the server to the home agent (Leung, col 7, lines 33-50), since the security associations may comprise keys (Leung, col 7, line 67), this uses a session key management protocol.

Wherein the at least one management client is included in an application device Mobile node is the individual computing device (Abstract).

Leung does not explicitly teach **requests to create and manage;** however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate

SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶0066.

In regard to **claim 18**, Leung discloses:

Leung discloses managing security associations or authentication services (handled by the server's internet protocol security services) and receive in return a security association (Leung, col 7, lines 16-32). The response is sent by the server to the home agent (Leung, col 7, lines 33-50), since the security associations may comprise keys (Leung, col 7, line 67), this uses a session key management protocol.

Leung discloses an interaction between a Home Agent the application device comprising management clients, that is connected to a server (the service device) via a communications network (Leung, col 6, lines 24-26) and one or more wireless clients. The Home Agent may contact the server with a request for services such as creating (Leung, col 2, line 58 to column 3, line 16).

Leung does not explicitly teach **requests to create and manage;** however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶0066.

In regard to **claim 19,** Leung discloses:

- wherein said communicating comprises communicating at least one of said security association management requests issued from said application device and corresponding responses via an interface associated with said application device (Leung col 6, lines 24-26), a server (the service device) via a communications network and one or more wireless clients.

In regard to **claim 20**, claim 18 is incorporated and Leung discloses:

- wherein said issuing comprises issuing said security association management requests comprising at least one of adding requests for adding security associations, deleting requests for deleting security, and querying requests for querying about security associations (Leung, col 6, lines 26-28 and col 8, lines 37-39), wherein security associations must be copied from the server to the Home Agent in order to create and manage or facilitate modifications in security associations.

In regard to **claim 21**, Leung discloses:

- providing one or more internet protocol security services comprising at least one of authentication services and encryption services from an internet protocol security service unit, wherein said internet protocol security service unit is deployed in a service device (Leung, col 6, lines 29-36, "In addition to providing a centralized server which is capable of storing security-associations for multiple Home Agents, the centralized server may provide further services. By way of example, the centralized server may provide authentication services and/or authorization services. While authentication determines who an entity is, authorization determines what services a user is allowed to perform, or access");

Leung does not explicitly teach **- receiving means for receiving security association management requests to create and manage security association, the security association management requests issued from at least one management client included in an application device external to said apparatus and for responding, in connection with said internet protocol security service means, to said received security association management requests**; however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012). Mobile node is the individual computing device (Abstract).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶0066.

In regard to **claim 22**, Leung discloses:

- providing one or more internet protocol security services comprising at least one of authentication services and encryption services from an internet protocol security service unit, said internet protocol security service unit being deployed in a service device (Leung, col 6, lines 29-36, "In addition to providing a centralized server which is capable of storing security-associations for multiple Home Agents, the centralized server may provide further services. By way of example, the centralized server may provide authentication services and/or authorization services. While authentication determines who an entity is, authorization determines what services a user is allowed to perform, or access");

- issuing security association management requests to create and manage, with a session key management protocol, security associations for use by said provided internet protocol security services, from at least one management client, said at least one management client being deployed in an application device (Leung, col 7, lines 54-61, "The security association may be retrieved from the server each time mobile node 702 sends a fresh registration request. To reduce the effort associated with this, the security association may be temporarily loaded into memory (e.g., a portion of DRAM) of the Home Agent. In this manner, some transfers of security associations from the server to the Home Agent are eliminated");

- receiving in a management server said security association management requests issued from said at least one management client (Leung, col 7, lines 35-47, "At step 714, the server receives the packet identifying the mobile node (e.g., an authorization request packet) from the Home Agent. … ..appropriate format (e.g., a TACACS+ authorization reply packet) and includes the security association").

- responding, in connection with said internet protocol security service unit, to said security association management requests received at said management server, said management server being deployed in said service device, wherein said application device is connected to said service device by a communication network (Leung, col 4, lines 33-45, "While authentication determines who an entity is, authorization determines what services a user is allowed to perform, or access. … available at http://www.ietf.org/internet-drafts/draft-grant-tacacs-02.txt, describes").

Leung does not explicitly teach **requests to create and manage**; however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶0066.

In regard to **claim 23**, Leung discloses:

- issuing, from at least one management client deployed in an application device, security association management requests to create and manage, with a session key management protocol, security associations for use by one or more internet protocol

security services comprising at least one of authentication services and encryption services provided by an internet protocol security service unit external to said application device (Leung, col 7, lines 62-68, "A suitable algorithm for clearing security associations from the Home Agent's memory may be employed (e.g., a least recently used (LRU) algorithm). While this approach can reduce traffic between server and Home Agent--and thereby eliminate attendant delay--it must also account for modifications of security associations (e.g., keys) on the server");

- communicating at least one of said issued security association management requests to a management server external to said application device, said management server configured to respond to said security association management requests in connection with said internet protocol security service unit (Leung, col 10, lines 18-24, "an architecture having a single processor that handles communications as well as routing computations, etc. would also be acceptable. Further, other types of interfaces and media could also be used with the router. Still further, in some cases, the invention can be implemented on network devices other than routers").

Leung does not explicitly teach **requests to create and manage**; however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶0066.

In regard to **claim 24**, Leung discloses:

- providing one or more internet protocol security services comprising at least one of authentication services and encryption services from an internet protocol security service unit, said internet protocol security service unit being deployed in a service device (Leung, col 8, lines 17-26, "FIG. 8 is a process flow diagram illustrating the steps performed .. server are illustrated along vertical line 806. Again, the server is preferably an AAA server that can provide authorization and accounting services as well as authentication services");

Leung teaches **included in an application device** (Abstract). But Leung does not explicitly teach **- receiving means for receiving security association management requests to create and manage security association, the security association management requests issued from at least one management client included in an application device external to said apparatus and for responding, in connection with said internet protocol security service means, to said received security association management requests**; however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the security association disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶66.

In regard to **claim 25**, Leung discloses:

- managing means for issuing security association management requests to create and manage, with a session key management protocol, security associations for use by one or more internet protocol security services comprising at least one of authentication

services and encryption services provided by an internet protocol security service means external to said apparatus (Leung, col 7, lines 35-47, "At step 714, the server receives the packet identifying the mobile node (e.g., an authorization request packet) from the Home Agent…the security association").

- communicating means for communicating said issued security association management requests to a management server external to said apparatus, said management server configured to respond to said security association management requests in connection with said internet protocol security service means (Leung, col 10, lines 18-24, "an architecture having a single processor that handles communications as well as routing computations, etc. would also be acceptable. Further, other types of interfaces and media could also be used with the router. Still further, in some cases, the invention can be implemented on network devices other than routers").

- wherein the apparatus is included in an application device , wherein Mobile node is the individual computing device (Abstract).

Leung does not explicitly teach **requests to create and manage**; however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶0066.

In regard to **claim 26**, Leung discloses:

- **internet protocol security service means for providing one or more internet protocol security services comprising at least one of authentication services and encryption services** (Leung, col 6, lines 32-36, "the centralized server may provide authentication services and/or authorization services. While authentication determines who an entity is, authorization determines what services a user is allowed to perform, or access");

Leung does not explicitly teach - **receiving means for receiving security association management requests to create and manage security association, the security association management requests issued from at least one management included in an application device_client external to said apparatus and for responding, in connection with said internet protocol security service means, to said received security association management requests**; however in a relevant art Yokote teach create and manage (two types of request) receives with IPSec (Yokote, ¶0012).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the security association disclosed in Yokote, since the present invention provides for adaptive network security, SA security methods, or SA management factors, to ensure the integrity of the SA at a node. Based on the SA management protocol, the SA management server determines which methods are appropriate for the maintaining the SA. The management factors include: maintaining SA's based on priority of the SA's; maintaining protection of the cache for a MN based on overflow principles; employing a keep-alive negotiation to ensure reachability of other nodes for which SA's are being stored; employing delete notification with a keep-alive negotiation, to eliminate SA for which there is no match found; and employing a re-key process for a lost SA, stated by Yokote at ¶0066.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (See form "PTO-892 Notice of reference cited).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MONJOUR RAHIM whose telephone number is (571)270-3890. The examiner can normally be reached on 5:30 AM - 3:30 PM (Mo - Th).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz, Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Monjour Rahim/
Patent Examiner
Art Unit: 2434
Date: 06/23/2010

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434